

CLAIMS

What is claimed is:

- 1 1. In a video source device, a method comprising:
2 a video source application requesting from a video hardware interface status
3 with respect to a link linking said video source device to an external video sink
4 device, and supplementing said status request with a first basis value to a
5 symmetric ciphering/deciphering process;
6 the video source application receiving from said video hardware interface
7 said requested status and a verification key, generated through said symmetric
8 ciphering/deciphering process employing said first basis value; and
9 the video source application verifying the correctness of said verification key
10 to determine whether to trust said provided status.
- 1 2. The method of claim 1, wherein said method further comprises said video
2 source application supplementing said status request with a selection key for the
3 video hardware interface to use to generate an authentication key for use to
4 generate said verification key.
- 1 3. The method of claim 1, wherein said verification of the correctness of the
2 received verification key comprises said video source application independently
3 generating its own copy of the verification key.
- 1 4. The method of claim 3, wherein said independent generation of said video
2 source application's own copy of said verification key comprises said video source

3 application independently generating its own copy of an authentication key by
4 summing a plurality of cryptographic keys over a selection key received from said
5 video hardware interface.

1 5. The method of claim 3, wherein said independent generation of said video
2 source application's own copy of said verification key comprises said video source
3 application applying a one way function to at least a first selected subset of said first
4 basis value provided to said video hardware interface using an independently
5 generated copy of an authentication key.

1 6. The method of claim 5, wherein said independent generation of said video
2 source application's own copy of said verification key further comprises said video
3 source application applying said one way function to a selection key said video
4 hardware interface received from said video sink device for use by said video
5 hardware interface to authenticate said video sink device, using the result of said
6 first application of the one-way function.

1 7. The method of claim 6, wherein said independent generation of said video
2 source application's own copy of said verification key further comprises said video
3 source application applying said one way function to at least a second selected
4 subset of said first basis value provided to said video hardware interface using the
5 result of said second application of the one-way function.

1 8. The method of claim 6, wherein said independent generation of said video
2 source application's own copy of said verification key further comprises said video

1 13. The method of claim 11, wherein said independent generation of said video
2 source application's own copy of said ciphering key comprises said video source
3 application applying a one way function to at least a first selected subset of said
4 second basis value provided to said video hardware interface using an
5 independently generated copy of an authentication key.

1 15. In a video source device, a method comprising:
2 a video source application requesting from a video hardware interface a
3 secret employed by said video hardware interface to cipher video to be transmitted
4 by said video hardware interface to an external video sink device, and
5 supplementing said secret request with a basis value to said symmetric
6 ciphering/deciphering process;
7 the video source application receiving from said video hardware interface
8 said requested secret in a ciphered form, having been ciphered using a ciphering
9 key generated using said symmetric ciphering/deciphering process and employing
0 said basis value; and

11 the video source application deciphering said ciphered secret using an
12 independently generated copy of said ciphering key.

1 16. The method of claim 15, wherein said method further comprises said video
2 source application supplementing said secret request with a selection key for the
3 video hardware interface to use to generate an authentication key for use by said
4 symmetric ciphering/deciphering process.

1 17. The method of claim 15, wherein said method further comprises said video
2 source application independently generating its own copy of the ciphering key.

1 18. The method of claim 17, wherein said independent generation of said video
2 source application's own copy of said ciphering key comprises said video source
3 application independently generating an authentication key by summing a plurality
4 of cryptographic keys over a selection key received from said video hardware
5 interface.

1 19. The method of claim 17, wherein said independent generation of said video
2 source application's own copy of said ciphering key comprises said video source
3 application applying a one way function to at least a first selected subset of said
4 basis value provided to said video hardware interface using an independently
5 generated copy of an authentication key.

1 20. The method of claim 19, wherein said independent generation of said video
2 source application's own copy of said ciphering key further comprises said video
3 source application applying said one way function to at least a second selected

4 subset of said basis value provided to said video hardware interface using the result
5 of said first application of the one-way function.

1 21. In a video source device, a method comprising:

2 a video hardware interface receiving from a video source application a
3 request for status with respect to a link linking said video source device to an
4 external video sink device, and said status request being supplemented with a first
5 basis value to a symmetric ciphering/deciphering process;

6 the video hardware interface returning said requested status to said video
7 source application, and accompanying said returned requested status with a
8 verification key, generated using said symmetric ciphering/deciphering process and
9 employing said first basis value, to allow said video source application to determine
10 whether to trust said returned status.

1 22. The method of claim 21, wherein said method further comprises said video
2 hardware interface further accompanying said returned status with a selection key
3 for the video source application to use to independently generate its own copy of an
4 authentication key for use to independently generate its own copy of said verification
5 key.

1 23. The method of claim 21, wherein said generation of said verification key
2 comprises said video hardware interface generating an authentication key by
3 summing a plurality of cryptographic keys over a selection key received from said
4 video source application.

1 28. The method of claim 21, wherein said method further comprises
2 said video hardware interface receiving from said video source application
3 request for a secret employed by said video hardware interface to cipher video to be
4 transmitted by said video hardware interface to said external video sink device, said
5 secret request being also supplemented with a second basis value to said
6 symmetric ciphering/deciphering process; and

1 33. In a video source device, a method comprising

2 a video hardware interface receiving from a video source application request
3 for a secret employed by said video hardware interface to cipher video to be
4 transmitted by said video hardware interface to an external video sink device, said
5 secret request being supplemented with a basis value to a symmetric
6 ciphering/deciphering process; and

7 said video hardware interface returning said requested secret in a ciphered
8 form to said video source application, the secret having been ciphered by a
9 ciphering key generated using said symmetric ciphering/deciphering process and
10 employing said basis value.

1 34. The method of claim 33, wherein said method further comprises said video
2 hardware interface receiving from said video source application a selection key
3 supplementing said secret request for the video hardware interface to use to
4 generate an authentication key for use in said symmetric ciphering/deciphering
5 process.

1 35. The method of claim 33, wherein said generation of said ciphering key
2 comprises said video hardware interface generating an authentication key by
3 summing a plurality of cryptographic keys over a selection key received from said
4 video source application.

1 36. The method of claim 33, wherein said generation of said ciphering key
2 comprises said video hardware interface applying a one way function to at least a
3 first selected subset of said basis value using an authentication key.

1 37. The method of claim 36, wherein said generation of said ciphering key further
2 comprises said video hardware interface applying said one way function to at least a
3 second selected subset of said basis value using the result of said first application of
4 the one-way function.

1 38. An article of manufacture comprising:
2 a storage medium having stored therein a plurality of programming
3 instructions implementing a video source application that requests from a video
4 hardware interface status with respect to a link linking said video source device to
5 an external video sink device, and supplements said status request with a basis
6 value to a symmetric ciphering/deciphering process, when the programming
7 instructions are executed by a processor, the video source application, upon
8 receiving from said video hardware interface said requested status and a verification
9 key generated using said symmetric ciphering/deciphering process and employing
10 said basis value, further verifies the correctness of said verification key to determine
11 whether to trust said provided status.

1 39. The article of manufacture of claim 38, wherein as part of said verification of
2 the correctness of the received verification key, said video source application
3 independently generates its own copy of an authentication key by summing a
4 plurality of cryptographic keys over a selection key received from said video
5 hardware interface.

1 40. The article of manufacture of claim 38, wherein as part of said verification of
2 the correctness of the received verification key, said video source application
3 applies a one way function to at least a first selected subset of said basis value

4 provided to said video hardware interface using an independently generated copy of
5 an authentication key.

1 41. An article of manufacture comprising:

2 a storage medium having stored therein a plurality of programming
3 instructions implementing a video source application that requests from a video
4 hardware interface a secret employed by said video hardware interface to cipher
5 video to be transmitted by said video hardware interface to an external video sink
6 device, and supplements said secret request with a basis value to said symmetric
7 ciphering/deciphering process, when the programming instructions are executed by
8 a processor, the video source application, upon receiving from said video hardware
9 interface said requested secret in a ciphered form, having been ciphered using a
10 ciphering key generated using said symmetric ciphering/deciphering process and
11 employing said basis value, further deciphers said ciphered secret using an
12 independently generated copy of said ciphering key.

1 42. The article of manufacture of claim 41, wherein said video source application
2 independently generates its own copy of said ciphering key, including generation of
3 an authentication key by summing a plurality of cryptographic keys over a selection
4 key received from said video hardware interface.

1 43. The article of manufacture of claim 41, wherein said video source application
2 independently generates its own copy of said ciphering key, including application of
3 a one way function to at least a first selected subset of said basis value provided to
4 said video hardware interface, using an independently generated copy of an
5 authentication key.

1

2

5

5

1

1

4 said video hardware interface using an independently generated copy of an
5 authentication key.

1 47. An apparatus comprising:

2 a video hardware interface equipped to securely transmit digital video to an
3 external video sink device coupled to said apparatus by way of said video hardware
4 interface;

5 a storage medium having stored therein a plurality of programming
6 instructions implementing a video source application that requests from said video
7 hardware interface a secret employed by said video hardware interface to cipher
8 video to be transmitted by said video hardware interface to said external video sink
9 device, and supplements said secret request with a basis value to said symmetric
10 ciphering/deciphering process, when the programming instructions are executed,
11 the video source application, upon receiving from said video hardware interface said
12 requested secret in a ciphered form, having been ciphered using a ciphering key
13 generated using said symmetric ciphering/deciphering process and employing said
14 basis value, further deciphers said ciphered secret using an independently
15 generated copy of said ciphering key; and

16 a processor coupled to said storage medium and said video hardware
17 interface to execute said programming instructions.

1 48. The apparatus of claim 47, wherein said video source application
2 independently generates its own copy of said ciphering key, including generation of
3 an authentication key by summing a plurality of cryptographic keys over a selection
4 key received from said video hardware interface.

- 1 49. The apparatus of claim 47, wherein said video source application
- 2 independently generates its own copy of said ciphering key, including application of
- 3 a one way function to at least a first selected subset of said basis value provided to
- 4 said video hardware interface using an independently generated copy of an
- 5 authentication key.

09540190-033100
DO NOT WRITE IN THESE SPACES